

【特許請求の範囲】

【請求項1】 ネットワークに接続された複数のコンピュータノードに分散して記憶された一群の機密情報のいずれかに対するアクセス要求を実行するか否かを管理するための前記一群の機密情報に共通に設けられたアクセス管理プログラムであって、

前記一群の機密情報のうち、前記アクセス管理プログラムにアクセスしてきたユーザに割り当てられたアクセスレベルに対応してあらかじめ定められた少なくとも一つの機密情報に前記ネットワークを介してアクセスするための少なくとも一つのアクセスメソッドを含むアクセスオブジェクトを当該ユーザに対応して生成し、
前記少なくとも一つの機密情報に対する前記ユーザからのアクセス要求を受け付け、前記少なくとも一つのアクセスメソッドを用いて当該少なくとも一つの機密情報にアクセスする、
ステップをコンピュータに実行させることを特徴とするアクセス管理プログラム。

【請求項2】 前記生成するステップは、複数のアクセスレベルに対応してあらかじめ生成された、オブジェクトを生成するための複数のファクトリのうち、前記ユーザに割り当てられたアクセスレベルに対応する一つのファクトリにより、前記アクセスオブジェクトを生成することを特徴とする請求項1に記載のアクセス管理プログラム。

【請求項3】 前記複数のファクトリは、前記アクセス管理プログラムを実行時に記憶するためのメモリと異なる記憶手段にあらかじめ記憶され、
前記生成するステップは、
前記一つのファクトリが前記記憶手段から前記メモリに既にロードされているか否かを判別し、
当該ファクトリがまだロードされていないと判断されたとき、前記記憶手段から前記メモリに当該ファクトリをロードし、
前記ロードされたファクトリにより前記アクセスオブジェクトを生成する、
ステップを含むことを特徴とする請求項2記載のアクセス管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークに接続された複数のコンピュータノードに分散して記憶された一群の機密情報のいずれかに対するアクセス要求を実行するか否かを管理するためのアクセス管理プログラム、アクセス管理システム、アクセス管理方法に関する。

【0002】

【従来の技術】 従来、ネットワークに接続された複数のコンピュータノードに実装された一群の機密情報管理サ

ーバプログラムが複数の機密情報サービスを提供し、ユーザがこれらの機密情報サービスをネットワークを介して利用できるようになっている。ユーザにあらかじめアクセスレベルを割り当て、アクセスレベルに応じてユーザが利用できる機密情報サービスを制限する方法が一般に取られている。アクセスレベルと当該アクセスレベルのユーザがアクセス権限を有する機密情報サービスとの関係は、コンピュータシステムのシステム管理者によりあらかじめ定められ、アクセスポリシーとも呼ばれる。

【0003】 ユーザによる機密情報サービスの利用の可否を制御するためにアクセス管理サーバプログラムが上記複数の機密情報管理サーバプログラムに共通に設けられ、ユーザはいずれかの機密情報サービスを使用するときには、まず当該アクセス管理サーバプログラムにアクセスする。当該アクセス管理サーバプログラムが、ユーザが遅んだ機密情報サービスを利用する権限を有するか否かを当該ユーザのアクセスレベルに基づいて判断し、ユーザが当該機密情報サービスを利用する権限を有するときには、当該機密情報サービスを提供する機密情報管理サーバプログラムへアクセスしていた。

【0004】

【発明が解決しようとする課題】 しかしながら、従来技術では、アクセスポリシーの変更あるいは利用可能な一群の機密情報管理サーバプログラムに関する変更、追加、削除（以下、システム構成の変更とも呼ぶ）が生じたとき、機密情報管理サーバプログラムをその変更に合わせてするために多くのプログラム変更作業を要していた。

【0005】 したがって、本発明の目的は、アクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成の変更時に、その変更と比較的簡単に適合させるのに適したアクセス管理プログラムを提供することである。

【0006】

【課題を解決するための手段】 上記目的を達成するために、本発明に係るアクセス管理プログラムは、ネットワークに接続された複数のコンピュータノードに分散して記憶された一群の機密情報のいずれかに対するアクセス要求を実行するか否かを管理するための前記一群の機密情報に共通に設けられたアクセス管理プログラムであって、前記一群の機密情報のうち、前記アクセス管理プログラムにアクセスしてきたユーザに割り当てられたアクセスレベルに対応してあらかじめ定められた少なくとも一つの機密情報に前記ネットワークを介してアクセスするための少なくとも一つのアクセスメソッドを含むアクセスオブジェクトを当該ユーザに対応して生成し、前記少なくとも一つの機密情報に対する前記ユーザからのアクセス要求を受け付け、前記少なくとも一つのアクセスメソッドを用いて当該少なくとも一つの機密情報にアクセスする、ステップをコンピュータに実行させるもので

ある。

【0007】このようにアクセスレベルに対応して定められたアクセスオブジェクトをユーザに対応して生成して使用することにより、アクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成が変更されたとき、ユーザ対応に生成する上記アクセスオブジェクトに含まれるメソッドを変更するように、アクセス管理プログラムを変更するという比較的簡単な作業により、アクセスポリシー又はシステム構成の変更にアクセス管理プログラムを適合させることができる。

【0008】具体的には、前記生成するステップは、複数のアクセスレベルに対応してあらかじめ生成された、オブジェクトを生成するための複数のファクトリのうち、前記ユーザに割り当てられたアクセスレベルに対応する一つのファクトリにより、前記アクセスオブジェクトを生成する。

【0009】このようにアクセスレベルに対応して定められたアクセスオブジェクトを生成するためのファクトリを用いることにより、アクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成の変更時にファクトリを更新するという比較的簡単な作業によりアクセス管理プログラムをアクセスポリシー又はシステム構成の変更に適合させることができる。

【0010】更に具体的には、前記複数のファクトリは、前記アクセス管理プログラムを実行時に記憶するためのメモリと異なる記憶手段にあらかじめ記憶され、前記生成するステップは、前記一つのファクトリが前記記憶手段から前記メモリに既にロードされているか否かを判別し、当該ファクトリがまだロードされていないと判断されたとき、前記記憶手段から前記メモリに当該ファクトリをロードし、前記ロードされたファクトリにより前記アクセスオブジェクトを生成する、ステップを含む。

【0011】これにより、アクセスポリシー又はシステム構成の変更時に前記記憶手段に記憶されたファクトリを変更するというより簡単な方法により、アクセスポリシー又はシステム構成の変更にアクセス管理プログラムを適合させることができる。

【0012】

【発明の実施の形態】以下、本発明に係るアクセス管理プログラムの実施の形態を図面を参照して詳細に説明する。

【0013】図1は、本発明に係るアクセス管理プログラムの一つの実施の形態を用いたコンピュータシステムのブロック図である。図において、10、20、21、22、30、40、50、60は、コンピュータノードであり、例えばLAN70のようなネットワークに接続されている。本コンピュータシステムは例えば企業等の団体の内部で使用されるシステムである。

【0014】コンピュータノード10は、例えばワーク

ステーションにより構成される。より具体的には、コンピュータノード10は、メモリ11、表示装置12、中央処理装置(CPU)13、キーボード及びマウス等のポインティングデバイスを備える入力装置14、補助記憶装置15、これらを接続するバス16と、バス16とLAN70とを接続するネットワークインターフェースカード17よりなる。他のノードコンピュータも同様であるが、図には他のノードコンピュータに関しては当該ノードコンピュータのメモリに記憶されたプログラムあるいはデータのみを簡単化のために示している。

【0015】コンピュータノード10は、アクセス管理サーバプログラム100を実行する。コンピュータノード20、21、22は、機密情報サービスを提供する機密情報管理サーバプログラム20A、21A、22Aをそれぞれ実行する。これらのプログラムは、機密情報を含むデータベースをコンピュータノードに内蔵された図示しない補助記憶装置に記憶して管理する。機密情報管理サーバプログラムが実行されるコンピュータノードの数は一つ又は複数であればよく、その数は特に制限されないが、図には一例として3つのコンピュータノード20、21、22が示されている。

【0016】コンピュータノード30は、ディレクトリサーバプログラム31を実行する。ディレクトリサーバプログラム31は、複数のユーザに関する個人情報群31Aと後に述べるオブジェクトを生成するためのオブジェクトである複数のファクトリを内部に含むファクトリテーブル31B等を、内蔵する補助記憶装置(図示せず)に階層構造を用いて記憶し管理する。コンピュータノード40は、システム管理オブジェクト41及びファクトリ更新オブジェクト42を実行する。これらのオブジェクトは、アクセスポリシー又はシステム構成の変更時にコンピュータシステムのシステム管理者によりアクセス管理サーバプログラム100の更新のために使用される。

【0017】コンピュータノード50は、本コンピュータシステムのためのネームサーバプログラム51を実行する。コンピュータノード60は、機密情報管理サーバプログラム20A、21A、22A等を利用するユーザにより使用されるクライアントプログラム61を実行する。クライアントプログラム61をインストールしたコンピュータノードは実際には複数個存在するが、図には簡単化のための一つのコンピュータノード60のみを示す。本コンピュータシステムは、各コンピュータノード内の各プログラムがオブジェクトにより構成されている分散オブジェクトシステムを実現している。

【0018】本コンピュータシステムでは、ユーザにはあらかじめ複数のアクセスレベルの一つが割り当てられ、各アクセスレベルに対応して、アクセスが許される一つ又は複数の機密情報が定められている。具体的に、各アクセスレベルに対応して、機密情報管理サーバ

プログラム 20A、21A、22Aのうちアクセスが許される一つ又は複数の機密情報管理サーバプログラムがあらかじめ定められている。すなわち、機密情報管理サーバプログラム 20A、21A、22Aに対する各ユーザのアクセス権限は、当該ユーザに割り当てられたアクセスレベルに依存して定められている。アクセスレベルと当該アクセスレベルのユーザがアクセスを許される機密情報管理サーバプログラムとの関係（アクセスポリシー）は、コンピュータシステムのシステム管理者によりあらかじめ定められる。

【0019】本発明に係るアクセス管理プログラムの一つの実施の形態は、アクセス管理サーバプログラム 100、個人情報群 31A、ファクトリテーブル 31B、システム管理オブジェクト 41、ファクトリ更新オブジェクト 42により実現されている。本発明に係るアクセス管理システムの一つの実施の形態は、コンピュータノード 10、30、40とそれらに実装されたプログラムにより実現される。各ユーザは、機密情報管理サーバプログラム 20A、21A、22Aのいずれかにより提供される機密情報サービスを利用したいとき、クライアントプログラム 61を介してアクセス管理サーバプログラム 100にアクセスする。

【0020】アクセス管理サーバプログラム 100は、ユーザの認証を行い、ユーザの正当性を確認した後に、当該ユーザにアクセス権限が与えられた一つ又は複数の機密情報管理サーバプログラムにより管理されている機密情報に対するユーザのアクセス要求を受け付け、当該機密情報管理サーバプログラムと当該ユーザが使用するクライアントプログラム 61との間の通信を中継する。当該ユーザにアクセス権限が与えられていない他の機密情報管理サーバプログラムにより管理されている機密情報に対するアクセス要求は受け付けられない。

【0021】より具体的には、当該ユーザがアクセス権限を有しない一つ又は複数の機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを有し、当該ユーザがアクセス権限を有しない機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを有しないアクセスオブジェクトを当該ユーザに対応して生成し、このアクセスオブジェクトを用いてユーザがアクセス権限を有する機密情報管理サーバプログラムへのアクセスを実行し、当該機密情報管理サーバプログラムとユーザが使用するクライアントプログラムとの間の通信を中継する。

【0022】コンピュータシステムの運用の過程で、アクセスポリシーが変更されることがある。すなわち、あるアクセスレベルについて、当該アクセスレベルを有するユーザがアクセス権限を与えられていた機密情報管理サーバプログラムに対してアクセス権限が与えられなくなったり、あるいはその逆のことが起きる。あるいはアクセスレベルが追加されたり削減されたりすることが生

じる。

【0023】さらにはシステム構成が変更されることがある。すなわち、本コンピュータシステムで利用可能な機密情報管理サーバプログラムが変更、追加又は削除されたり、あるいはそれらが実装されるコンピュータノードが変更になることがある。

【0024】アクセスポリシーの変更又はシステム構成の変更が発生したとき、コンピュータノード 40に対するシステム管理者の指示入力にしたがって、各ユーザに対応して生成する上記アクセスオブジェクトとして、変更後のアクセスポリシー又は変更後のシステム構成に対応したアクセスオブジェクトが生成される。

【0025】アクセス管理サーバプログラム 100は、図示するように、コンピュータノード 10のメモリ 11に実装されたメインオブジェクト 80、認証オブジェクト 81、ファクトリ起動オブジェクト 82、コンテンツ生成オブジェクト 83、複数のファクトリ 84、アクセスオブジェクト 85、コンテンツオブジェクト 86等により構成される。複数のファクトリ 84は、それぞれ一つのアクセスレベルに対応して定められている。アクセスオブジェクト 85とコンテンツオブジェクト 86は、アクセス管理サーバプログラム 100にアクセスしたユーザに対応して生成される。

【0026】分散オブジェクトシステムを実現するためのオブジェクトアダプタ 87、オブジェクトリクエストブローカ 88等のオブジェクトもメモリ 11に実装される。これらのオブジェクトは共通オブジェクトリクエストブローカアーキテクチャ（CORBA）により定義されているオブジェクトである。オブジェクトアダプタ 87は、後述するオブジェクトレファレンスを決定する機能を有し、オブジェクトリクエストブローカ 88は、異なるオブジェクト間の通信路を提供する。コンピュータノード 10を制御するOSもメモリ 11に実装されるが、本OSは簡単化のために図示されていない。

【0027】なお、他のコンピュータノード 20、21、22、30、40、50、60にもオブジェクトアダプタ、オブジェクトリクエストブローカが実装されるが、これらのオブジェクトは簡単化のために図示されていない。他のコンピュータノードに実装されるOSについても同様である。

【0028】図2は、アクセス管理サーバプログラム 100により実行される一例としての処理の流れの概要を模式的に示す。アクセス管理サーバプログラム 100は、メインオブジェクト 80を起動することにより起動される。メインオブジェクト 80は、起動されると、認証オブジェクト 81、ファクトリ起動オブジェクト 82、コンテンツ生成オブジェクト 83を生成する。ユーザは、クライアントプログラム 61を介して認証オブジェクト 81にアクセスする（ステップ S1）。

【0029】認証オブジェクト 81は、ユーザの個人認

10

20

30

40

50

証を行うオブジェクトであり、ユーザが入力した識別情報に基づいてディレクトリサーバプログラム31により管理される当該ユーザの個人情報を読み出す(ステップS2)。ディレクトリサーバプログラム31は、個人情報群31Aとして、例えば複数のユーザの各々の電子証明書とそれに関連する情報及び他の個人情報を記憶する。ディレクトリサーバプログラム31は、例えばディレクトリ標準ITU X.500にしたがって情報を記憶する。

【0030】ユーザはユーザ認証情報として上記ディレクトリ標準で定められた当該ユーザの識別名(Distinguished Name -DN)を入力する。識別名(DN)は、例えばユーザの所属部署、氏名、電子メールアドレス等を含む。読み出された個人情報には、電子証明書に関連する情報その他の個人情報の他に、ユーザに割り当てられたアクセスレベルと、ユーザにあらかじめ割り当てられた他のユーザ識別情報(例えばユーザIDとパスワードの組)が含まれている。当該他の識別情報は、後に機密情報管理サーバプログラムが行う個人認証に使用される。

【0031】認証オブジェクト81は、ユーザが入力したユーザの識別名(DN)と読み出された個人情報とを用いて当該ユーザの正当性を確認し、ユーザの正当性が確認されると、認証オブジェクト81は、ファクトリ起動オブジェクト82を呼び出す(ステップS3)。このとき、ユーザに割り当てられたアクセスレベルと前述の他のユーザ識別情報とが引き渡される。

【0032】ファクトリ起動オブジェクト82は、引き渡されたアクセスレベルに対応するファクトリ84を呼び出す。すべてのアクセスレベルに対応する複数のファクトリ84は、ディレクトリサーバプログラム31が管理するファクトリテーブル31B内にあらかじめ格納されていて、各ファクトリ84は、メモリ11にロードされてから起動される。ファクトリ起動オブジェクト82は、内部にロード済みファクトリテーブル820を有する。ロード済みファクトリテーブル820は、各アクセスレベルに対応するファクトリ84がメモリ11に既にロードされているか否かを示すデータを保持している。

【0033】ファクトリ起動オブジェクト82は、起動されたときに、ユーザのアクセスレベルに対応するファクトリ84がメモリ11にロードされているか否かをこのロード済みファクトリテーブル820を参照して判断し、そのファクトリがまだメモリ11にロードされていないときには、ファクトリテーブル31Bからメモリ11にそのファクトリ84をロードし(ステップS4)、起動する(ステップS5)。そのファクトリ84が既にメモリ11にロードされているときには、ファクトリ起動オブジェクト82は、そのロード済みのファクトリ84を起動する(ステップS5)。起動時に前述の他のユーザ識別情報が引き渡される。

【0034】起動されたファクトリ84は、対応するアクセスレベルを有するユーザがアクセス権限を有する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを有するアクセスオブジェクト85を生成する(ステップS6)。このとき、ファクトリ84から前述の他のユーザ識別情報がアクセスオブジェクト85に引き渡される。こうして特定のユーザに対応してアクセスオブジェクト85が生成される。

【0035】このアクセスオブジェクト85の参照値は、ファクトリ84からファクトリ起動オブジェクト82に戻され(ステップS7)、更にファクトリ起動オブジェクト82から認証オブジェクト81に戻される(ステップS8)。ここで、オブジェクトの参照値は、当該オブジェクトが存在するコンピュータノード上に存在する他のオブジェクトが当該オブジェクトを特定するために使用されるオブジェクト識別情報である。認証オブジェクト81は、コンテンツ生成オブジェクト83にこの参照値を指定して、コンテンツオブジェクトの生成を要求し(ステップS9)、コンテンツ生成オブジェクト83は、ユーザに対応してコンテンツオブジェクト86を生成する(ステップS10)。

【0036】コンテンツオブジェクト86は、本コンピュータシステムで提供される複数の機密情報サービスのメニューをクライアントプログラム61に通知する機能と、いずれかの機密情報サービスがユーザにより選ばれたときに、その機密情報サービスを実行する機密情報管理サーバプログラムへの接続要求を当該ユーザのためのアクセスオブジェクト85に通知する機能を有する。

【0037】コンテンツ生成オブジェクト83は、コンテンツオブジェクト86が生成されると、認証オブジェクト81にコンテンツオブジェクト86の参照値を戻す(ステップS11)。認証オブジェクト81は、コンテンツオブジェクト86のオブジェクトレファレンスをクライアントプログラム61に通知する(ステップS12)。ここでオブジェクトのオブジェクトレファレンスは、当該オブジェクトが存在するコンピュータノードと異なるコンピュータノード上に存在する他のオブジェクトが当該オブジェクトを特定するために使用されるオブジェクト識別情報である。

【0038】クライアントプログラム61は、通知されたオブジェクトレファレンスを用いてコンテンツオブジェクト86を呼び出し、メニュー表示を要求する(ステップS13)。コンテンツオブジェクト86は、クライアントプログラム61に機密情報サービスのメニューリストデータを送る(ステップS14)。クライアントプログラム61は、このメニューリストデータに基づいて機密情報サービスの一覧を示すメニューを表示装置の画面に表示する。

【0039】ユーザが画面上の操作によりいずれかの機密情報サービスを選択すると、クライアントプログラム

61は、選択された機密情報サービスへの接続をコンテンツオブジェクト86に要求する(ステップS15)。コンテンツオブジェクト86は、この要求を当該ユーザに対応するアクセスオブジェクト85に通知する(ステップS16)。

【0040】アクセスオブジェクト85は、ユーザがアクセス権限を有する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを内蔵している。ユーザが要求した機密情報サービスを提供する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドがアクセスオブジェクト85に含まれている場合には、アクセスオブジェクト85はそのアクセス要求を受け付け、そのアクセスメソッドを実行し、当該機密情報管理サーバプログラムに接続する(ステップS17)。

【0041】ユーザがアクセス権限を有しない機密情報管理サーバプログラムにアクセスするためのアクセスメソッドは、アクセスオブジェクト85には内蔵されていない。したがって、ユーザが選択した機密情報サービスを提供する機密情報管理サーバプログラムに対してユーザがアクセス権限を有しない場合、アクセスオブジェクト85は、当該機密情報サービスに対するユーザの機密情報利用要求を受け付けない。

【0042】ステップS17により機密情報管理サーバプログラムがアクセスされた場合、当該機密情報管理サーバプログラムがユーザの識別情報の入力要求したときには、アクセスオブジェクト85内の上記アクセスメソッドは、ファクトリ84から引き継いだ前述の他のユーザ識別情報を当該機密情報管理サーバプログラムに転送する。ユーザの正当性が当該機密情報管理サーバプログラムにより認証されると、クライアントプログラム61とユーザが選択した機密情報サービスを提供する機密情報管理サーバプログラムとの間でアクセスオブジェクト85、コンテンツオブジェクト86を介した通信路が開かれることになる。

【0043】当該機密情報管理サーバプログラムは、応答情報をアクセスオブジェクト85に戻し(ステップS18)、アクセスオブジェクト85は、その応答情報をコンテンツオブジェクト86に戻し(ステップS19)、コンテンツオブジェクト86は、その情報をクライアントプログラム61に戻す(ステップS20)。クライアントプログラム61に対してその後ユーザが当該機密情報管理サーバプログラムに転送すべき情報を入力した場合には、当該情報は、同様にして当該機密情報管理サーバプログラムに転送される。

【0044】このようにしてクライアントプログラム61とユーザが選択した機密情報サービスを提供する機密情報管理サーバプログラムとの間でアクセスオブジェクト85、コンテンツオブジェクト86を介したデータ通信が実行されることになる。

【0045】他のユーザに関しても同様に対応するアク

セスオブジェクトとコンテンツオブジェクトが生成され、当該他のユーザが使用するクライアントプログラムと当該他のユーザが選択した機密情報を管理する機密情報管理サーバプログラムとの間でデータ通信が、上記データ通信と独立にかつ並行して実行されることになる。

【0046】なお、アクセスポリシーあるいはシステム構成の変更が生じたとき、アクセス管理サーバプログラム100がコンピュータノード40を用いてシステム管理者により更新される。具体的には、システム管理オブジェクト41、ファクトリ更新オブジェクト42を用いて、アクセスポリシーあるいはシステム構成の変更に伴い、変更されるべき又は不要になったファクトリがディレクトリサーバプログラム31内のファクトリテーブル31B及びメモリ11から削除され、変更後のファクトリあるいは新たに必要になったファクトリがファクトリテーブル31Bに追加される。

【0047】したがって、その後はあるアクセスレベルに対応するファクトリがメモリ11に存在しないときに、当該ファクトリはファクトリテーブル31Bからメモリ11にロードされることになり、ファクトリの変更、削除、追加等の更新が円滑に実現される。その結果、アクセスポリシー又はシステム構成の変更に適したアクセスオブジェクトを生成することが比較的容易になる。

【0048】以下では、アクセス管理サーバプログラム100と関連する他のプログラムの処理の詳細を説明する。図3から図6は、組み合わせてアクセス管理サーバプログラム100により実行される一例としての処理の概略フローチャートを示す。

【0049】まず、クライアントプログラム61は、アクセス管理サーバプログラム100へのアクセスをユーザから指示されると、認証オブジェクト81を呼び出す(ステップS101)。クライアントプログラム61は、この呼び出しに当たり分散オブジェクトシステムで通常行われる方法により認証オブジェクト81のオブジェクトレファレンスを取得し、上記呼び出しは取得されたオブジェクトレファレンスを用いて行われる。

【0050】例えば、クライアントプログラム61は、そのプログラムが実装されているコンピュータノード60内のオブジェクトリクエストブローカ62(図1)に、コンピュータノード50に実装されたネームサーバプログラム51へのアクセスを要求する。オブジェクトリクエストブローカ62は、この要求に応答して通信オブジェクトを生成し、クライアントプログラム61にその通信オブジェクトの参照値を戻す。

【0051】クライアントプログラム61は、生成された通信オブジェクトに認証オブジェクト81のオブジェクトレファレンスを要求する。生成された通信オブジェクトは、ネームサーバプログラム51に認証オブジェクト81のオブジェクトレファレンスを要求する。ネーム

サーバプログラム51は、認証オブジェクトに対応してあらかじめ記憶してあったオブジェクトレファレンスを上記通信オブジェクトに戻し、当該通信オブジェクトはそのオブジェクトレファレンスをクライアントプログラム61に戻す。こうして、クライアントプログラム61は呼び出すべき認証オブジェクト81のオブジェクトレファレンスを取得することができる。

【0052】認証オブジェクト81は、クライアントプログラム61により呼び出されると、内部のメソッドを実行してクライアントプログラム61にユーザ識別情報10を要求する(ステップS102)。認証は、ディレクトリサーバプログラム31により管理される複数のユーザに対してあらかじめ記憶された個人情報群を用いて行われる。各ユーザの個人情報には、例えば図3内に示すように、当該ユーザが使用する電子証明書の認証に使用される個人情報310を用いることができる。

【0053】電子証明書には例えばISO/IEC/ITUが定めたX.509電子証明書を使用することができる。すなわち、各ユーザの個人情報310は、電子証明書そのものとそれに関連する識別名(DN)その他の複数の情報及び他の個人情報を含む。電子証明書の証明に用いられる識別名(DN)は、その証明書を使用するユーザを特定するユーザ識別情報である。識別名(DN)は、例えばユーザの所属部署、氏名、電子メールアドレス等を含む。個人情報310に含まれる当該他の個人情報には、ユーザに割り当てられたアクセスレベル及び当該ユーザの他のユーザ識別情報(ユーザID及びパスワード)が含まれる。

【0054】このように個人情報310が前述のディレクトリ標準X.500にしたがって管理される場合、上記識別情報要求ステップS102においては、認証オブジェクト81は、例えば上記ディレクトリ標準で定められたユーザの識別情報である識別名(DN)の入力をクライアントプログラム61に要求する。ユーザが自己の識別名(DN)を入力すると、クライアントプログラム61が入力されたユーザ識別名(DN)を認証オブジェクト81に引き渡す(ステップS103)。

【0055】認証オブジェクト81は、入力された識別名(DN)を有する個人情報をディレクトリサーバプログラム31から取得する(ステップS104)。認証オブジェクト81は、取得された個人情報を用いて高度の安全性を有する認証プロトコルに基づいてクライアントプログラム61と通信してユーザの認証を行う(ステップS105)。このときクライアントプログラム61も適宜応答する(ステップS106)。上記認証プロトコルには例えばチャレンジ応答プロトコルを使用することができる。

【0056】アクセス管理サーバプログラム100は、上記個人認証において上記認証プロトコルに代えて、上記ユーザIDとパスワードを用いた認証も行ってもよい

が、上記認証プロトコルを用いることにより、通信の傍受等を防止することができ、より安全に個人認証を行うことができる。

【0057】ユーザが個人認証に合格しなかった場合(ステップS107)、認証オブジェクト81は、アクセス拒否をクライアントプログラム61に通知する(ステップS108)。一方、ユーザが認証に合格すると(ステップS107)、認証オブジェクト81は、ファクトリ起動オブジェクト82を呼び出す(ステップS109)。このとき、認証オブジェクト81は、ユーザの個人情報310に含まれたアクセスレベルと前述の他のユーザ識別情報(ユーザIDとパスワード)をファクトリ起動オブジェクト82に引き渡す。

【0058】図7は、ファクトリ起動オブジェクト82の例を模式的に示す。ファクトリ起動オブジェクト82は、メソッドとしてファクトリロードメソッド82Aとロード済みファクトリ更新メソッド82Bを含み、属性値としてロード済みファクトリテーブル820を含む。ロード済みファクトリテーブル820は、各アクセスレベルに対応するファクトリがメモリ11にロード済みか否かを示すテーブルである。

【0059】図8は、ロード済みファクトリテーブル820の例を示す。ロード済みファクトリテーブル820には、各アクセスレベルに対応して、アクセスレベルを記憶する領域821と、対応するファクトリの参照値を記憶する領域822が設けられる。あるアクセスレベルに対応するファクトリがメモリ11にロードされたときには、当該アクセスレベルに対応して当該ファクトリの参照値が参照値記憶領域822に記憶される。しかし、そのアクセスレベルに対応するファクトリがメモリ11にロードされていないときには、当該アクセスレベルに対応する参照値記憶領域822には、それ以外の値、例えば「0」が記憶されたままである。

【0060】図では、アクセスレベル「1」と「3」に対しては対応するファクトリが既にロードされ、当該ファクトリの参照値を例示する値「AAAA」と「BBBB」が記憶され、アクセスレベル「2」と「4」に対しては対応するファクトリがロードされていないことを示す値「0」が参照値記憶領域822に記憶されている。

【0061】図4において、ファクトリ起動オブジェクト82は、認証オブジェクト81により呼び出されると、ファクトリロードメソッド82Aを起動する。このファクトリロードメソッド82Aは、ロード済みファクトリテーブル820を参照して認証オブジェクト81より通知されたユーザのアクセスレベルに対応するファクトリがメモリ11にロード済みであるか否かを判別する(ステップS110)。

【0062】もしそのファクトリがまだメモリ11にロードされていないと判断されたときには(ステップS111)、ディレクトリサーバプログラム31(図1)が

管理するファクトリテーブル31Bから、当該ファクトリをメモリ11にロードし(ステップS112)、ロードされたファクトリの参照値をファクトリテーブル820(図8)内のユーザのアクセスレベルに対応する参照値記憶領域822にセットする(ステップS113)。

【0063】その後、当該ファクトリ84を呼び出す(ステップS114)。このとき、ファクトリ起動オブジェクト82は、前述の他のユーザ識別情報(ユーザIDとパスワード)を当該ファクトリに引き渡す。一方、ステップS111において、ユーザのアクセスレベルに対応するファクトリ84が既にメモリ11にロード済みであると判断された場合には、ステップS112からS113は実行されず、ステップS114が実行される。

【0064】図9は、ファクトリ84の例を模式的に示す。ファクトリ84は、メソッドとしてアクセスオブジェクト生成メソッド84Aと対応するアクセスレベルのユーザがアクセス権限を有する一つ又は複数の機密情報管理サーバプログラムをそれぞれアクセスするための一つ又は複数のアクセスメソッド(今の例では複数のアクセスメソッド84B、84C)を含む。

【0065】アクセスメソッド84B、84Cは、それぞれの属性値として対応する機密情報管理サーバプログラムと通信するための通信制御情報を含む。通信制御情報には、例えば当該機密情報管理サーバプログラムが実装されたコンピュータノードのIPアドレスと当該コンピュータノード内のポート番号と当該コンピュータノードと通信するための通信用デバイスドライバの名称が含まれている。

【0066】ファクトリ84は、オブジェクト属性値としてアクセスレベル841、アクセスイネーブルリスト842、アクセスディスエーブルリスト843を更に含む。アクセスレベル841は、当該ファクトリが対応するアクセスレベルを示し、アクセスイネーブルリスト842は、当該アクセスレベルのユーザがアクセス権限を有する一つ又は複数の機密情報管理サーバプログラムを示す。アクセスディスエーブルリスト843は、当該アクセスレベルのユーザがアクセス権限を有しない一つ又は複数の機密情報管理サーバプログラムを示す。

【0067】図にはこれらの属性の値の例を括弧内に示している。アクセスレベル841が例えば「2」であり、アクセスイネーブルリスト842は、ユーザがアクセス権限を有する機密情報管理サーバプログラムとして機密情報管理サーバプログラム#1(20A)と機密情報管理サーバプログラム#3(22A)を示し、アクセスディスエーブルリスト843は、ユーザがアクセス権限を有しない機密情報管理サーバプログラムとして機密情報管理サーバプログラム#2(21A)を示している。

【0068】図4に戻り、ファクトリ84は、ファクトリ起動オブジェクト82により呼び出されると、アクセ

スオブジェクト生成メソッド84Aを実行し、当該メソッドによりユーザ用のアクセスオブジェクト85を生成する(ステップS115)。

【0069】図10は、アクセスオブジェクト85の例を模式的に示す。アクセスオブジェクト85は、メソッドとしてユーザがアクセス権限を有する一つ又は複数の機密情報管理サーバプログラムをそれぞれアクセスするための一つ又は複数のアクセスメソッド(今の例では複数のアクセスメソッド85A、85B)を含む。これらのアクセスメソッド85A、85Bは、ファクトリ84内のアクセスメソッド84B、84Cと同じである。

【0070】すなわち、ファクトリ84のアクセスオブジェクト生成メソッド84Aは、ステップS115においてアクセスオブジェクト85を生成するときに、ファクトリ84内のメソッド84B、84Cをアクセスオブジェクト85内にコピーしてアクセスオブジェクト85内のアクセスメソッド85A、85Bを生成する。したがって、アクセスメソッド85A、85Bは、それぞれの属性値としてアクセスメソッド84B、84Cの属性値と同じ通信制御情報を含む。

【0071】アクセスオブジェクト85は、オブジェクトの属性値としてアクセスレベル851、アクセスイネーブルリスト852、アクセスディスエーブルリスト853、ユーザIDとパスワード854を更に含む。アクセスレベル851、アクセスイネーブルリスト852、アクセスディスエーブルリスト853は、ファクトリ84の属性値841から843(図9)と同じである。

【0072】すなわち、ファクトリ84のアクセスオブジェクト生成メソッド84Aは、ステップS115(図4)においてアクセスオブジェクト85を生成するときに、ファクトリ84内のアクセスレベル841、アクセスイネーブルリスト842、アクセスディスエーブルリスト843をアクセスオブジェクト85内にコピーする。属性値としてのユーザIDとパスワード854には、ファクトリ起動オブジェクト82からファクトリ84に引き渡された引数が使用される。

【0073】図4に戻り、起動されたファクトリ84は、生成されたアクセスオブジェクト85の参照値をファクトリ起動オブジェクト82に戻す(ステップS116)。ファクトリ起動オブジェクト82は、認証オブジェクト81にアクセスオブジェクト85の参照値に戻す(ステップS117)。

【0074】図5を参照するに、認証オブジェクト81は、コンテンツ生成オブジェクト83を呼び出し、引数としてアクセスオブジェクト85の参照値を引き渡す(ステップS118)。コンテンツ生成オブジェクト83は、コンテンツオブジェクト86を生成し(ステップS119)、生成されたコンテンツオブジェクト86の参照値を認証オブジェクト81に戻す(ステップS120)。

【0075】図11は、コンテンツ生成オブジェクト83の例を模式的に示す。コンテンツ生成オブジェクト83は、メソッドとしてコンテンツ生成メソッド83Aと、メインメニューリスト提供メソッド83Bと、複数の機密情報サービス利用メソッド83C、83D、…とを含み、属性値としてメインメニューリストデータ831を含む。

【0076】機密情報サービス利用メソッド83C、83D、…は、本コンピュータシステムで利用可能な複数の機密情報管理サーバプログラム#1(20A)、#2(21A)、#3(22A)(図1)により提供される全機密情報サービスのいずれかを利用するためのメソッドである。メインメニューリストデータ831は、これらの全機密情報サービスの名称等をクライアントプログラム61に提示するためのデータである。

【0077】図12は、メインメニューリストデータ831の例を示す。メインメニューリストデータ831は、機密情報サービスの名称831Aと機密情報サービス利用メソッド名831Bとの対を本コンピュータシステムで利用可能な全機密情報サービスに対して含む。機密情報サービス利用メソッド名831Bには、コンテンツ生成オブジェクト83(図11)に含まれた機密情報サービス利用メソッド83C、83D、…のうち記憶領域831Aに記憶された機密情報サービスの名称に対応するメソッドの名称が使用される。

【0078】例えば機密情報サービスの名称として「勤休表登録」が含まれ、コンテンツ生成オブジェクト83内に含まれた対応する機密情報サービス利用メソッドの名称として「勤休表登録メソッド」が含まれる。このメインメニューリストデータ831の使用方法は後に説明する。

【0079】図13は、コンテンツオブジェクト86の例を模式的に示す。コンテンツオブジェクト86は、メソッドとしてメインメニューリスト提供メソッド86Aと、複数の機密情報サービス利用メソッド86B、86C、…とを含み、属性値としてメインメニューリストデータ861を含む。メインメニューリスト提供メソッド86A、機密情報サービス利用メソッド86B、86C、…は、コンテンツ生成オブジェクト83内のメソッド83B、83C、83D、…と同じである。

【0080】コンテンツ生成オブジェクト83は、認証オブジェクト81から呼ばれると、コンテンツ生成メソッド83Aを実行する。前述のステップS119及びS120はコンテンツ生成メソッド83Aにより実行される。コンテンツ生成メソッド83Aは、ステップS119においてコンテンツオブジェクト86を生成するとき、コンテンツ生成オブジェクト83内のメソッド83B、83C、83D、…をコンテンツオブジェクト86内にコピーしてコンテンツオブジェクト86内のメソッド86A、86B、86C、…を生成する。

【0081】同様に、コンテンツ生成オブジェクト83内のメインメニューリストデータ831をコピーしてコンテンツオブジェクト86内の属性値としてメインメニューリストデータ861を生成する。更にコンテンツ生成オブジェクト83は、アクセスオブジェクト85の参照値862をコンテンツオブジェクト86の属性値として組み込む。コンテンツ生成メソッド83Aは、その後、コンテンツオブジェクト86の参照値を認証オブジェクト81に戻すステップS120を実行する。

10 【0082】図5に戻り、認証オブジェクト81は、オブジェクトアダプタ87(図1)を呼び出し、コンテンツオブジェクト86の参照値を引き渡してオブジェクトレファレンスの生成を要求する(ステップS121)。オブジェクトアダプタ87からコンテンツオブジェクト86のオブジェクトレファレンスを受け取り(ステップS122)、クライアントプログラム61にこのオブジェクトレファレンスを戻す(ステップS123)。

20 【0083】図6において、クライアントプログラム61は、戻されたオブジェクトレファレンスを用いてコンテンツオブジェクト86を呼び出す(ステップS124)。コンテンツオブジェクト86は、クライアントプログラム61から呼び出されると、メインメニューリスト提供メソッド86A(図13)を起動する。起動されたメインメニューリスト提供メソッド86Aは、メインメニューリストデータ861をクライアントプログラム61に戻す(ステップS125)。

30 【0084】クライアントプログラム61は、戻されたメインメニューリストデータ861に基づいて、図14に例示するように、そこに含まれた機密情報サービスの名称の一覧をメインメニューとして表示装置の画面に表示する(ステップS126)。ユーザが表示されたいずれかの機密情報サービスの名称を選ぶと、クライアントプログラム61は、その名称のサービスを利用するためのメソッドを呼び出す(ステップS127)。具体的には、クライアントプログラム61は、ユーザが選択した機密情報サービスの名称に対応してメインメニューリストデータ861に含まれた機密情報サービス利用メソッドの名称を指定してコンテンツオブジェクト86を呼び出す。

40 【0085】コンテンツオブジェクト86では、指定された名称の機密情報サービス利用メソッド、例えば86Bが起動され、この機密情報サービス利用メソッドが、アクセスオブジェクト85の参照値862(図13)を用いてアクセスオブジェクト85を呼び出し、当該機密情報サービス利用メソッドに対応して定められた、当該機密情報サービス利用メソッドが利用する機密情報サービスを提供する機密情報管理サーバプログラムにアクセスするためのアクセスメソッドを呼び出す(ステップS128)。

50 【0086】例えば、ユーザが機密情報サービスとして

勤休表登録を選んだ場合、コンテンツオブジェクト 86 内の当該サービスを利用するためのメソッド、例えば 86B (図 13) が起動され、起動されたメソッド 86B は、当該機密情報サービスを提供する機密情報管理サーバプログラム、例えば 20A (図 1) にアクセスするためのアクセスメソッド、例えば 85A (図 10) を呼び出す。

【0087】アクセスオブジェクト 85 は、呼び出されたアクセスメソッド 85A が内部に存在するか否かを判断し (ステップ S129)、そのアクセスメソッドが存在する場合には、当該呼び出しを受け付ける、すなわちユーザのアクセス要求を受け付ける。すなわちそのアクセスメソッドの属性値である通信制御情報に含まれた IP アドレス、ポート番号、通信用のデバイスドライバを用いて当該機密情報管理サーバプログラム、例えば 20A にアクセスする。

【0088】こうしてクライアントプログラム 61 と当該機密情報管理サーバプログラム 20A との間で、コンテンツオブジェクト 86 内の機密情報サービス利用メソッド 86B 及びアクセスオブジェクト 85 内のアクセスメソッド、例えば 85A を経由した通信路が形成される。

【0089】上記アクセスメソッド 85A は、機密情報管理サーバプログラム 20A からユーザ識別情報の入力求められたときには、アクセスオブジェクト 85 の属性値として記憶された前述のユーザ識別情報 (ユーザ ID とパスワード) 854 (図 10) をユーザに代わって機密情報管理サーバプログラム 20A に送信する。

【0090】機密情報管理サーバプログラム 20A による個人認証が成功すると、上記アクセスメソッド 85A は、当該機密情報管理サーバプログラムからの戻り値 (応答情報) をコンテンツオブジェクト 86 内の機密情報サービス利用メソッド 86B に戻す (ステップ S130)。当該機密情報サービス利用メソッド 86B は、戻り値をクライアントプログラム 61 に戻す (ステップ S132)。

【0091】その後、ユーザがクライアントプログラム 61 に機密情報サービスを利用するためのデータを入力すると、当該データは、コンテンツオブジェクト 86 内の上記機密情報サービス利用メソッド 86B 及びアクセスオブジェクト 85 内の上記アクセスメソッド 85A を経由して上記機密情報管理サーバプログラム 20A に転送され、再度機密情報管理サーバプログラム 20A から戻り値が上記通信路を経てクライアントプログラム 61 に戻される。

【0092】このようにして、ユーザはクライアントプログラム 61 を介してアクセス権限を有する機密情報管理サーバプログラムが提供する機密情報サービスを利用することができる。ユーザによる機密情報サービスの利用が終了するとアクセス管理サーバプログラム 100 及

びクライアントプログラム 61 の処理が終了する。ユーザによるいずれかの機密情報管理サーバプログラムの使用が終了すると、当該ユーザ用のアクセスオブジェクト 85 及びコンテンツオブジェクト 86 はメモリ 11 から削除される。

【0093】ステップ S128 によりアクセスオブジェクト 85 内のアクセスメソッドがコンテンツオブジェクト 86 内の機密情報サービス利用メソッドにより呼び出されたときに、当該アクセスメソッドがアクセスオブジェクト 85 内に存在しない場合 (ステップ S129)、アクセスオブジェクト 85 は、当該呼び出しを受け付けず、すなわちユーザのアクセス要求を受け付けず。

【0094】具体的には、アクセスオブジェクト 85 は、ユーザが選択した機密情報サービスを利用できない旨をコンテンツオブジェクト 86 内の呼び出し元の機密情報サービス利用メソッドに戻す (ステップ S131)。当該機密情報サービス利用メソッドは、その戻り値をクライアントプログラム 61 に戻し (ステップ S132)、アクセス管理サーバプログラム 100 の処理が終了する。こうしてユーザがアクセス権限を有しない機密情報管理サーバプログラムへのアクセスは禁止される。

【0095】このようにユーザに対応してアクセスオブジェクト 85 及びコンテンツオブジェクト 86 が生成され、これらのオブジェクトを用いてユーザのアクセス権限の有無、すなわちアクセス要求がユーザがアクセス権限を有する機密情報に対するものであるかが判断される。ユーザがアクセス権限を有する場合、これらのオブジェクトを用いてユーザが要求した機密情報を管理する機密情報管理サーバプログラムとユーザが利用するクライアントプログラムの間で通信路が形成される。

【0096】したがって、各ユーザによる機密情報へのアクセス権限のチェックとアクセスが、他のユーザに対する同様の処理と独立にかつ並行に実行される。その結果、各ユーザのアクセス権限のチェックとアクセスを他のユーザに対する同様の処理の影響を受けないで効率よく実行できる。

【0097】なお、アクセスポリシーあるいはシステム構成の変更が生じたとき、アクセス管理サーバプログラム 100 がコンピュータノード 40 を用いてシステム管理者により以下のようにして更新される。

【0098】システム管理オブジェクト 41 には、アクセスポリシーを示すアクセスポリシー表及び機密情報管理サーバプログラムの構成を示すシステム構成表を属性値として含んでいる。

【0099】図 15 は、アクセスポリシー表 401 の例を示す。アクセスポリシー表 401 は、使用可能なアクセスレベルの各々に対して、当該アクセスレベルのユーザが各機密情報管理サーバプログラムに対してアクセス権限を有する否かのフラグを保持している。図ではフラ

グ値「1」がアクセス権限があることを示し、「0」がアクセス権限がないことを示す。

【0100】例えば、アクセスレベル「1」のユーザは、機密情報管理サーバプログラム#1から#3のいずれに対してアクセス権限を有するが、アクセスレベル「2」のユーザは、機密情報管理サーバプログラム#1と#3に対してアクセス権限を有し、機密情報管理サーバプログラム#2に対してはアクセス権限を有しないことが示されている。

【0101】なお、アクセスポリシーの変更態様には、あるアクセスレベルに対するアクセス権限が変更される場合がある。あるアクセスレベル自体が削除される場合もある。さらにはアクセスレベルが追加される場合もある。

【0102】図16は、システム構成表402の例を示す。システム構成表402は、使用可能な機密情報管理サーバプログラムの各々に対して当該機密情報管理サーバプログラムにアクセスするために使用される通信制御情報を保持している。通信制御情報には、例えば当該機密情報管理サーバプログラムが実装されたコンピュータノードのIPアドレスと当該コンピュータノード内のポート番号と当該コンピュータノードと通信するための通信デバイスドライバの名称が含まれている。

【0103】システム構成の変更態様には、ある機密情報管理サーバプログラムが変更される場合、すなわち、当該機密情報管理サーバプログラムの通信制御情報が変更される場合がある。あるいは機密情報管理サーバプログラムが削除される場合もある。さらには機密情報管理サーバプログラムが追加される場合もある。

【0104】図17はシステム管理オブジェクト41の処理の一例の概略フローチャートを示す。システム管理オブジェクト41は、システム管理者により起動されると、システム管理者の要求に応じて上記アクセスポリシー表401及びシステム構成表402を表示装置の画面に表示し、アクセスポリシーとシステム構成の変更入力を受け付け（ステップS411）、削除すべきファクトリ及び追加すべきファクトリを指定してファクトリ更新オブジェクト42にそれぞれのファクトリの削除又は追加を要求する（ステップS412）。

【0105】削除すべきファクトリと追加すべきファクトリは変更入力に基づいて判別される。既にあるファクトリが新たなファクトリにより置換されるべきときには、元のファクトリの削除と新たなファクトリの追加が必要となる。なお、追加すべきファクトリは、システム管理者により本コンピュータシステムとは別のところで事前に生成してコンピュータノード40内に記憶させておき、後にファクトリの更新を実行するときに当該追加すべきファクトリをファクトリテーブル31Bに移動すればよい。しかし、追加すべきファクトリをシステム管理オブジェクト41により自動的に生成させることが

より望ましい。

【0106】アクセスポリシーの変更態様とファクトリの更新態様との関係は以下のとおりである。あるアクセスレベルのアクセス権限が変更されたときには、当該アクセスレベルを有するユーザに対して生成するアクセスオブジェクト85（図10）内に含まれるアクセスメソッド及び属性値を変更する必要がある。したがって、当該アクセスオブジェクトの生成に用いる、当該アクセスレベルに対応するファクトリを新たなファクトリにより置換する必要がある。

【0107】あるアクセスレベル自体が削除された場合には、当該アクセスレベルに対応するファクトリを削除する必要がある。あるアクセスレベルが追加された場合には、当該アクセスレベルに対応するファクトリを追加する必要がある。

【0108】システム構成の変更態様とファクトリの更新態様との関係は以下のとおりである。ある機密情報管理サーバプログラムが変更されたとき、すなわち、当該機密情報管理サーバプログラムの通信制御情報が変更されたときには、当該機密情報管理サーバプログラムに対するアクセス権限を有するアクセスレベルに対応するファクトリをすべて新たなファクトリにより置換する必要がある。あるいは機密情報管理サーバプログラムが削除された場合もあるいは新たに追加された場合も同様である。

【0109】図18は、ファクトリ更新オブジェクト42の処理の一例の概略フローチャートを示す。ファクトリ更新オブジェクト42は、システム管理オブジェクト41により起動されると、ディレクトリサーバプログラム31内のファクトリテーブル31Bに含まれたファクトリを更新する、すなわち、ファクトリを削除するか又はそこに新たなファクトリをコンピュータノード40から追加する（ステップS421）。

【0110】その後、ファクトリ更新オブジェクト42は、システム構成の変更がなされたか否かを判断する（ステップS422）。システム構成の変更がなされた場合には、後に説明するようにメインオブジェクト80を新たなメインオブジェクトにより置換し、当該新たなメインオブジェクトを再起動する必要がある。その場合には、メモリ11にロード済みのファクトリ等はすべて削除されるので、以下に述べる処理は実行されず、ファクトリ更新オブジェクト42は終了する。

【0111】ステップS422においてシステム構成の変更がないと判断された場合には、ファクトリ起動オブジェクト82内のロード済みファクトリ更新メソッド82B（図7）にロード済みのファクトリの一部の削除とロード済みファクトリテーブル820の更新を要求する（ステップS423）。

【0112】削除されるべきファクトリは、ディレクトリサーバプログラム31内のファクトリテーブル31B

から削除されたファクトリのうちメモリ 11 にロード済みのファクトリである。すなわち、新たなファクトリにより置換されるべきファクトリ又は不要になったファクトリであって、メモリ 11 にロード済みのファクトリである。ファクトリ起動オブジェクト 82 内のロード済みファクトリ更新メソッド 82B は、指定されたファクトリをメモリ 11 から削除する。

【0113】更に、ロード済みファクトリ更新メソッド 82B は、当該削除されたファクトリに対するアクセスレベルが削除されていない場合には、ロード済みファクトリテーブル 820 (図 8) の、上記削除されたファクトリに対応するアクセスレベルに対する参照値記憶領域 822 に値「0」を記憶する。アクセスレベルが削除された場合には、ロード済みファクトリテーブル 820 内の当該アクセスレベルに対応する参照値記憶領域 822 にアクセスレベルの削除を示す値、例えば「-1」を記憶する。あるいは、ロード済みファクトリテーブル 820 内の当該アクセスレベルを記憶する領域 821 と、対応する参照値記憶領域 822 を削除してもよい。

【0114】アクセスレベルが追加された場合には、ロード済みファクトリテーブル 820 内に当該アクセスレベルを記憶する領域 821 と、対応する参照値記憶領域 822 を追加し、追加された領域 821 に追加されたアクセスレベルを記憶し、追加された参照値記憶領域 822 に、ロードされていないことを示す値「0」を格納する。こうしてファクトリ更新オブジェクト 42 は終了する。

【0115】図 17 に戻り、システム管理オブジェクト 41 は、ファクトリ更新オブジェクト 42 による処理が終了すると、システム構成の変更がなされたか否かを判断する (ステップ S413)。システム構成の変更がなされていないときには、システム管理オブジェクト 41 は終了する。

【0116】こうして、ファクトリ起動オブジェクト 82 は、アクセスポリシーの変更後も、メモリ 11 にロードされていないファクトリをディレクトリサーバプログラム 31 内のファクトリテーブル 31B から、アクセスしてきたユーザのアクセスレベルに対応するファクトリをロードするだけでよいことになる。

【0117】一方、ステップ S413 においてシステムの構成が変更されたと判断されたときには、後に述べる理由により使用中のメインオブジェクト 80 を新たなメインオブジェクトにより置換し、当該新たなメインオブジェクトを再起動する (ステップ S414)。当該新たなメインオブジェクトは、システム管理者が事前にコンピュータノード 40 内に準備しておけばよい。しかし、システム管理オブジェクト 41 により新たなメインオブジェクトを自動的に生成することがより望ましい。

【0118】新たなメインオブジェクトが再起動されると、使用中であった認証オブジェクト 81、ファクトリ

起動オブジェクト 82、コンテンツ生成オブジェクト 83、ロード済みのファクトリ 84、生成済みのアクセスオブジェクト 85、コンテンツオブジェクト 86 は削除され、新たに認証オブジェクト 81、ファクトリ起動オブジェクト 82、コンテンツ生成オブジェクト 83 が生成される。

【0119】メインオブジェクトの更新と再起動が必要な理由は以下のとおりである。システム構成の変更に伴い、利用可能な機密情報サービスが変更される。例えば、機密情報管理サーバプログラムが追加された場合には、その機密情報管理サーバプログラムにより提供される機密情報サービスを利用するために新たな機密情報サービス利用メソッドをコンテンツ生成オブジェクト 83 内のメソッドとして追加することが必要となる。併せてメインメニューリストデータ 831 の内容も増やすことになる。

【0120】あるいは、システム構成の変更に伴い、既に利用可能な機密情報サービスが他の機密情報サービスにより置換された場合、当該既にあった古い機密情報サービスを利用するための、コンテンツ生成オブジェクト 83 内に含まれていた特定の機密情報サービス利用メソッドを新たな機密情報サービス利用メソッドにより置換する必要が生じる。併せて、メインメニューリストデータ 831 内の当該古い機密情報サービスに関連するデータを新たな機密情報サービスに関連するデータで置換する必要が生じる。

【0121】したがって、システム構成が変更されたときには、使用中のコンテンツ生成オブジェクト 83 及びそこから生成されたコンテンツオブジェクト 86 を更新する必要がある。コンテンツオブジェクト 86 は、コンテンツ生成オブジェクト 83 により生成され、コンテンツ生成オブジェクト 83 は、メインオブジェクト 80 により生成されるので、メインオブジェクト 80 自体を更新する必要がある。

【0122】以上のようにして、アクセスポリシーの更新及びシステム構成の変更時にアクセス管理サーバプログラム 100 をシステム管理者の制御の元で更新することができる。

【0123】このようにアクセス管理サーバプログラム 100 が使用するファクトリ 84 をディレクトリサーバプログラム 31 に格納し、アクセス管理サーバプログラム 100 がディレクトリサーバプログラム 31 からアクセス管理サーバプログラム 100 が使用するメモリ 11 にロードする方法を採ると、アクセスポリシーあるいはシステム構成の変更に必要なアクセス管理サーバプログラム 100 を適合させるために必要なアクセス管理サーバプログラム 100 の変更量が少なくなる。このことは、複数のアクセス管理サーバプログラムが異なるコンピュータノードに実装されている場合に特に有効である。

【0124】上記実施の形態では、個人情報と複数のフ

ファクトリをディレクトリサーバプログラム31により記憶された。このことは、以下の点で優れている。ディレクトリサーバプログラムは極めて容易にバイナリデータを保持することができる。したがって、ディレクトリサーバプログラム31は、バイナリデータである複数のファクトリを保持するのに適している。更に、企業の個人情報群は基本的には階層構造を有している。元々ディレクトリサーバプログラム31は情報をツリー構造を用いて階層構造で保存する。したがって、ディレクトリサーバプログラムは、個人情報群を階層的に保存するのに適している。

【0125】更に、ディレクトリサーバプログラム31は、電子証明書を含む個人情報を記憶しており、高度のセキュリティ機能を有する認証アルゴリズムにしたがって、アクセス管理サーバプログラム100のための個人認証を行うことができる。しかも、最近は多くの企業で個人情報をディレクトリサーバプログラムにより管理している。本実施の形態は、そのようなディレクトリサーバプログラムをファクトリの記憶にも共用しているので、新たなディレクトリサーバプログラムを使用しないで実現することができる。

【0126】なお、本発明は以上の実施の形態に限定されないことは言うまでもない。例えば、コンテンツ生成オブジェクト83及びコンテンツオブジェクト86に使用されたメインメニューリストデータ831(図11)又は861(図13)は、提供される機密情報サービスのすべてに関する機密情報サービスの名称等を含んでいた。

【0127】しかし、コンテンツオブジェクト86に含まれるメインメニューリストデータ861として、ユーザのアクセスレベルに対してアクセス権限が与えられない機密情報サービスに対するデータを含まないものを用いることもできる。このようなメインメニューリストデータは、あらかじめアクセスレベルに対応して生成しておけばよい。この場合には、ユーザにアクセス権限がない機密情報サービスをユーザが選択することはなくなる。このことにより当該機密情報サービスに対するユーザのアクセス要求を受け付けないようにしていることになる。

【0128】また、認証オブジェクト81による個人認証ではディレクトリ標準X.500により定められた識別名(DN)を用いたが、これに代えてユーザ認証情報とパスワードを用いて個人認証を行ってもよい。更に、機密情報管理サーバプログラム20Aを内蔵するコンピュータノード20等は、LAN70により接続された、企業等の団体の内部で使用されるものが例示されたが、当該コンピュータノード20等は、インターネットあるいは専用回線等で接続された遠方に位置するものでもよく、また、機密情報も企業等の団体内の個人に関する情

報でなくともよいことは言うまでもない。

【0129】

【発明の効果】以上に説明したように、本発明によればアクセスポリシー又は機密情報管理サーバプログラムに関するシステム構成の変更時に、その変更アクセス管理プログラムを比較的簡単に適合させることができる。

【図面の簡単な説明】

【図1】本発明に係るアクセスプログラムの一つの実施の形態を使用するコンピュータの概略構成図である。

【図2】アクセス管理サーバプログラムにより実行される一例としての処理の流れを模式的に示す図である。

【図3】アクセス管理サーバプログラムにより実行される一例としての処理の流れの一部の概略フローチャートである。

【図4】アクセス管理サーバプログラムにより実行される一例としての処理の流れの他の一部の概略フローチャートである。

【図5】アクセス管理サーバプログラムにより実行される一例としての処理の流れの更に他の一部の概略フローチャートである。

【図6】アクセス管理サーバプログラムにより実行される一例としての処理の流れの更に他の一部の概略フローチャートである。

【図7】ファクトリ起動オブジェクトの例を模式的に示す図である。

【図8】ロード済みファクトリテーブルの例を示す図である。

【図9】ファクトリの例を模式的に示す図である。

【図10】アクセスオブジェクトの例を模式的に示す図である。

【図11】コンテンツ生成オブジェクトの例を模式的に示す図である。

【図12】メインメニューリストデータの例を模式的に示す図である。

【図13】コンテンツオブジェクトの例を模式的に示す図である。

【図14】ユーザに対して表示される機密情報サービスの名称の一覧の例を示す図である。

【図15】アクセスポリシー表の例を示す図である。

【図16】システム構成表の例を示す図である。

【図17】システム管理オブジェクトの処理の一例の概略フローチャートである。

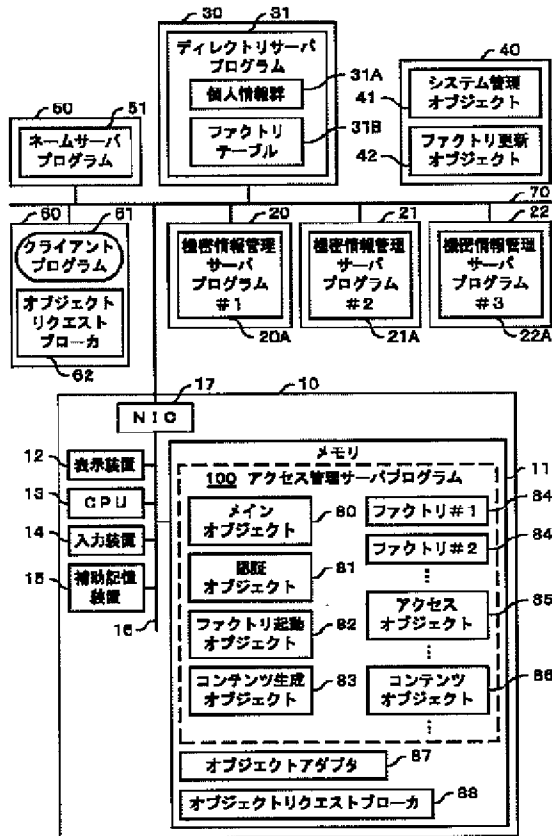
【図18】ファクトリ更新オブジェクトの処理の一例の概略フローチャートである。

【符号の説明】

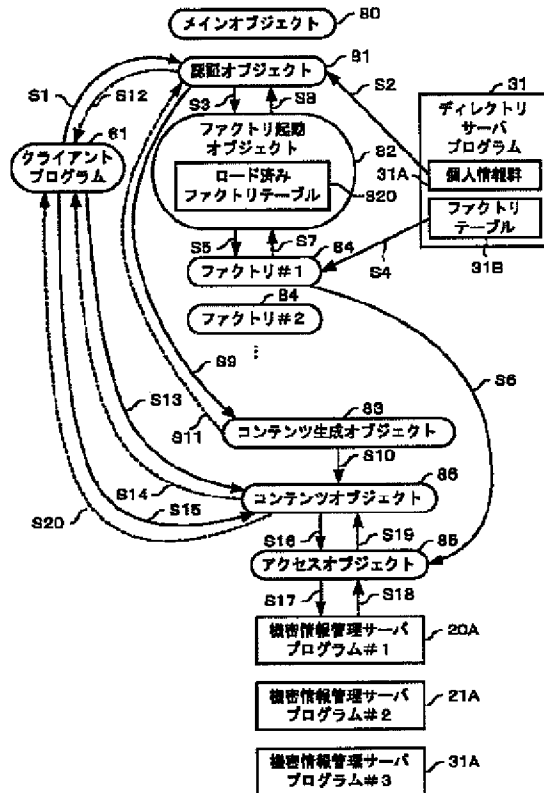
10、20、21、22、30、40、50、60…コンピュータノード

70…LAN

【図1】



【図2】



【図7】

82 ファクトリ起動オブジェクト

メソッド	ファクトリロードメソッド	82A
	ロード済みファクトリ更新メソッド	82B
属性値	ロード済みファクトリテーブル	82C

【図8】

820 ロード済みファクトリテーブル

アクセスレベル	参照値
1	AAAA
2	0
3	BBBB
4	0
!	!

【図14】

動作表登録

...

【図9】

84 ファクトリ

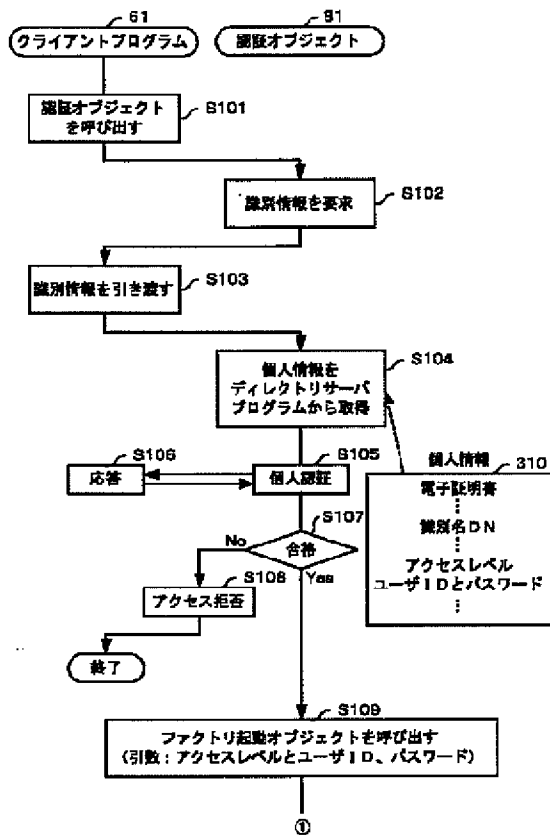
メソッド	アクセスオブジェクト生成メソッド	84A
	アクセスメソッド(機密情報管理サーバプログラム#1用)	84B
	アクセスメソッド(機密情報管理サーバプログラム#3用)	84C
属性値	アクセスレベル(2)	841
	アクセスイネーブルリスト(1, 3)	842
	アクセスディスエーブルリスト(2)	843

【図10】

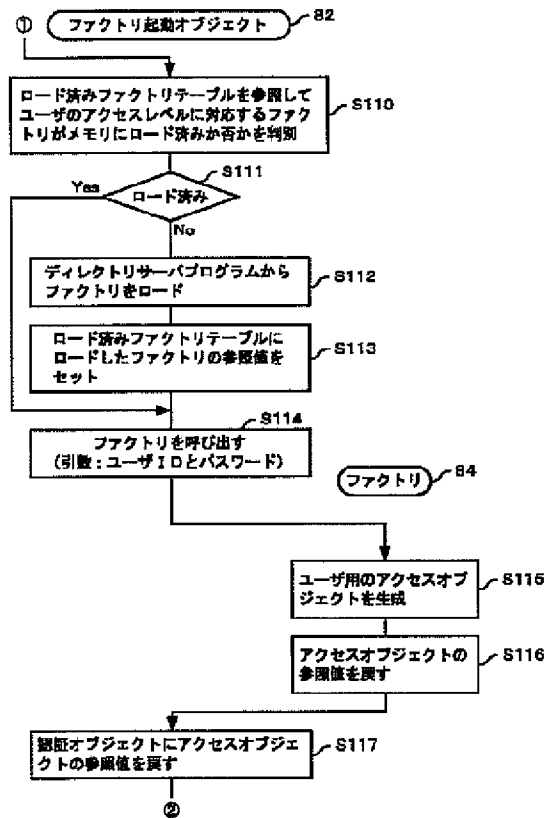
85 アクセスオブジェクト

メソッド	アクセスメソッド(機密情報管理サーバプログラム#1用)	85A
	アクセスメソッド(機密情報管理サーバプログラム#3用)	85B
属性値	アクセスレベル(2)	851
	アクセスイネーブルリスト(1, 3)	852
	アクセスディスエーブルリスト(2)	853
	ユーザIDとパスワード	854

【図3】



【図4】



【図11】

83 コンテンツ生成オブジェクト	
メソッド	コンテンツ生成メソッド 83A
	メインメニューリスト提供メソッド 83B
	機密情報サービス利用メソッド#1 83C
	機密情報サービス利用メソッド#2 83D
	⋮
属性値	メインメニューリストデータ 831

【図12】

831 メインメニューリストデータ	
機密情報サービス名 831A	機密情報サービス利用メソッド名 831B
勤休表登録	勤休表登録メソッド
⋮	⋮

【図15】

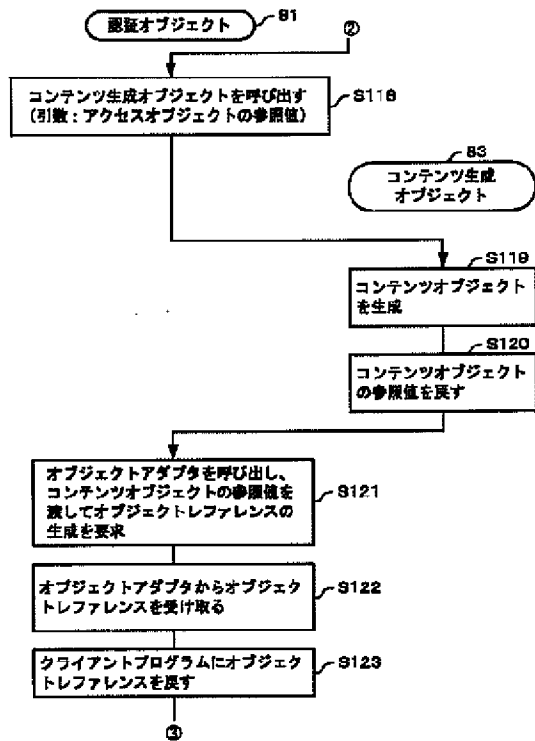
【図13】

86 コンテンツオブジェクト	
メソッド	メインメニューリスト提供メソッド 86A
	機密情報サービス利用メソッド#1 86B
	機密情報サービス利用メソッド#2 86C
	⋮
属性値	メインメニューリストデータ 861
	アクセスオブジェクトの参照値 862

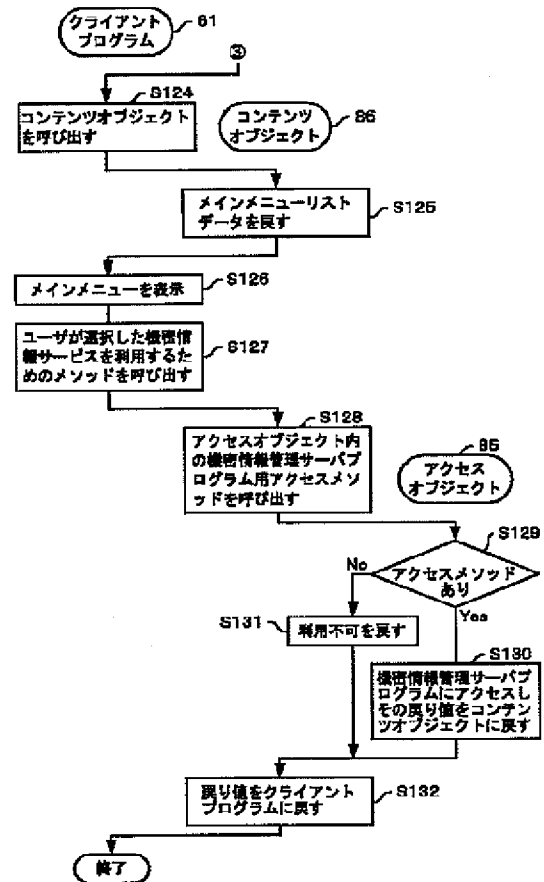
401 アクセスポリシー表

アクセスレベル	機密情報管理サーバプログラム		
	#1	#2	#3
1	1	1	1
2	1	0	1
⋮	⋮	⋮	⋮

【図5】



【図6】

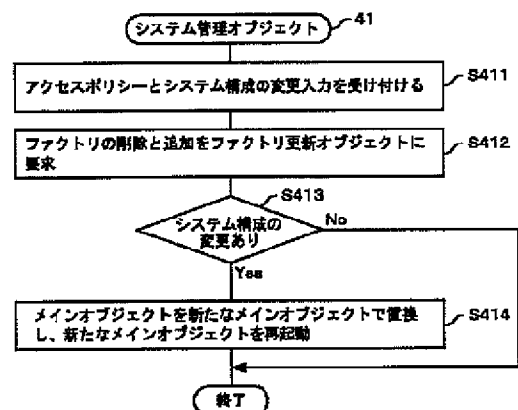


【図16】

422 システム構成表

機密情報管理 サーバプログラム	通信制御情報		
	IPアドレス	ポート番号	通信用デバイスドライバ の名称
#1			
#2			
#3			

【図17】



【図18】

